Relational Refinement Types for Higher-Order Shape Transformers

Suresh Jagannathan

Department of Computer Science, Purdue University, IN, US
suresh@cs.purdue.edu

Abstract

Understanding, discovering, and proving useful properties of sophisticated data structures are central problems in program verification. A particularly challenging exercise for shape analyses involves reasoning about sophisticated shape transformers that preserve the shape of a data structure (*e.g.*, the data structure skeleton is always maintained as a balanced tree) or the relationship among values contained therein (*e.g.*, the *in-order* relation of the elements of a tree or the *parent-child* relation of the elements of a heap) across program transformations.

In this talk, we consider the specification and verification of such transformers for ML programs. The structural properties preserved by transformers can often be naturally expressed as inductively-defined *relations* over the recursive structure evident in the definitions of the datatypes they manipulate. By carefully augmenting a refinement type system with support for reasoning about structural relations over algebraic datatypes, we realize an expressive yet decidable specification language, capable of capturing useful structural invariants, which can nonetheless be automatically verified using off-the-shelf type checkers and theorem provers. Notably, our technique generalizes to definitions of *parametric* relations for polymorphic data types which, in turn, lead to highly composable specifications over higher-order polymorphic shape transformers.

1998 ACM Subject Classification D.2.4 Software/Program Verification-Correctness proofs, Formal Methods, D.3.2 Applicative (Functional) Languages, F.3.1 Specifying and Verifying and Reasoning about Programs

Keywords and phrases Relational Specifications; Inductive and Parametric Relations; Refinement Types, Shape Analysis, Data Structure Verification

Digital Object Identifier 10.4230/LIPIcs.FSTTCS.2015.9

Category Invited Talk

35th IARCS Annual Conf. Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2015).
Editors: Prahladh Harsha and G. Ramalingam; pp. 9–9

Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany